Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A system for enabling remote access to an application server, ~~upon authentication of a location from which a user has sought access as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server,~~ the system comprising:

a means for enabling a user to request remote access to the application server;

a gaming card having security data for identifying the user;

an access server, for receiving and processing a request for access to the application server from ~~a user request enabling~~ the means for enabling a user to request remote access to the application server, the access server adapted to be located remote from the user's geographic location;

a card reader connected to the means for enabling a user to request access to the application server at the user's geographic location, wherein the card reader includes a time out feature that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the user's geographic location;

an authenticator for authenticating the geographic location of the user responsive to receipt of a processed request from the access server, the authenticator including a challenge and response system for authenticating the geographic location of the user and verifying an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data, and wherein the authenticator is adapted to be connected to the access server;

means for interconnecting the access server and the authenticator; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that determines a ~~physical~~ geographic location of an originating number to prevent the user from connecting to the access server from a ~~physical~~

geographic location other than the user's geographic location, and wherein the first number authenticating system relies on user input and does not rely on GPS.

2. (original) The system of claim 1, wherein the authenticator comprises an authenticating server.

3. (canceled)

4. (canceled)

5. (canceled)

6. (original) The system of claim 1, wherein the interconnecting means comprise a network.

7. (currently amended) The system of claim 2, wherein the authenticating server includes a database of authorized geographic locations, for enabling verification of the geographic location of the user as an authorized user geographic location.

8. (original) The system of claim 2, wherein the authenticating server comprises a Remote Access Dial-In User Service (RADIUS) server.

9. (canceled)

10. (canceled)

11. (currently amended) The system of claim 1[[5]], wherein the means for enabling a user to request remote access to the application server ~~enabling means comprise~~ includes an interface station.

12. (currently amended) The system of claim 1[[5]], wherein the means for enabling a user to request remote access to the application server ~~enabling means comprise~~ includes a client.

13. (currently amended) The system of claim 1[[5]], wherein the means for enabling a user to request remote access to the application server ~~enabling means include~~ includes a geographic location identifier.

14. (canceled)

15. (currently amended) The system of claim 1[[5]], wherein the ~~user request enabling~~ means for enabling a user to request remote access to the application server includes ~~include~~ an identifier associated with the user's geographic location, and the authenticator comprises means for authenticating the identifier associated with the user's geographic location.

16. (currently amended) The system of claim 1[[5]], wherein the ~~user request enabling~~ means for enabling a user to request remote access to the application server includes ~~include~~ a dialer[[,]] located at the user's geographic location, and wherein the dialer includes a number associated therewith.

17. (canceled)

18. (currently amended) The system of claim 1[[5]], wherein the interconnecting means are further adapted to interconnect the ~~user request enabling~~ means for enabling a user to request remote access to the application server.

19. (original) The system of claim 6, wherein the network comprises an intranet.

20. (original) The system of claim 6, wherein the network comprises the Internet.

21. (currently amended) The system of claim 8, further comprising means for enabling the user to request remote access to the application server, wherein the authenticating server is further adapted to issue a security challenge to the ~~user request enabling~~ means for enabling a user to request remote access to the application server.

22. (original) The system of claim 15, wherein the locating identifier comprises a cookie.

23. (currently amended) The system of claim 16, wherein the authenticator comprises a number identifier for identifying the number associated with the dialer located at the user's geographic location.

24. (currently amended) The system of claim 16, wherein a dialing system includes a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing

therefrom and each dialer associated with a different user's geographic location, and the authenticator further comprises means for identifying the first number dialed from in the dialing system.

25. (original) The system of claim 20, wherein the locating identifier comprises a dynamic cookie.

26. (currently amended) The system of claim 21, wherein the ~~user request enabling~~ means for enabling a user to request remote access to the application server is ~~are~~ adapted to issue a response to the security challenge, and the ~~authenticating means include~~ authenticator includes a database for enabling verification of the response of the ~~user request enabling~~ means for enabling a user to request remote access to the application server to the security challenge.

27. (original) The system of claim 23, wherein the number identifier comprises Automatic Number Identification.

28. (original) The system of claim 24, wherein the first number identifying means comprises Dialed Number Identification Services.

29. (currently amended) The system of claim 26, wherein the authenticator is further adapted to verify the response of the ~~user request enabling~~ means for enabling a user to request remote access to the application server to the security challenge based on the database in the authenticator, and to authorize access to the application server.

30. (currently amended) A system for enabling remote access to an application server, ~~upon authentication of a location from which a user has sought access as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server,~~ the system comprising:

a means for enabling a user to request remote access to the application server, wherein the user enabling means includes a dialer having a dialing number associated therewith;

a gaming card having security data for identifying the user;

an access server, for receiving and processing a request for access to the application server from a user request enabling means, the server adapted to be located remote from the user's geographic location;

a card reader connected to the user enabling means at the user's geographic location, wherein the card reader includes a time out feature that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the user's geographic location;

an authenticator for authenticating the geographic location of the user responsive to receipt of the processed request from the access server, the authenticator adapted to be connected to the access server, the authenticator including a Remote Access Dial-In Service (RADIUS) server and a challenge and response system for authenticating the geographic location of the user and verifying an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data;

means for interconnecting the access server and the authenticator;

~~means for enabling the user to request remote access to the application server, such means including a dialer, located at the user's~~ geographic ~~location, wherein the dialer includes a dialing number associated therewith; and~~

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that determines a ~~physical~~ geographic location of an originating number to prevent the user from connecting to the access server from a ~~physical~~ geographic location other than the user's geographic location, and wherein the first number authenticating system relies on user input and does not rely on GPS.

31. (currently amended) The system of claim 30, wherein the authenticator includes a number identifier for identifying the number associated with the dialer located at the user's geographic location.

32. (currently amended) The system of claim 30, and further comprising a dialing system including a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each associated with a different user's geographic location, and the authenticator comprises means for identifying the first number dialed from the dialing system.

33. (original) The system of claim 31, wherein the number identifier comprises Automatic Number Identification.

34. (original) The system of claim 32 wherein the first number identifying means comprises Dialed Number Identification Services.

35. (canceled)

36. (canceled)

37. (canceled)

38. (canceled)

39. (canceled)

40. (canceled)

41. (canceled)

42. (canceled)

43. (canceled)

44. (canceled)

45. (canceled)

46. (canceled)

47. (canceled)

48. (currently amended) A method of enabling remote access to an application server, ~~upon authentication of a location from which a user has sought access thereto as an authorized location, for enabling processing of a transaction requiring user location authentication, wherein the user location includes means for enabling the user to request remote access to the application server, in a system which comprises an access server, for receiving and processing a request for~~

~~access to the application server from user request enabling means, adapted to be located remote from the user's location, an authenticator for authenticating the identity and the location of the user responsive to receipt of the processed request from the access server, adapted to be connected to the access server, and means for interconnecting the access server and the authenticator, wherein~~ the method comprising ~~comprises~~:

requesting an access server to enable a user ~~at a user's location~~ to access an application server;

authenticating ~~the~~ a geographic location of the user via ~~the~~ an authenticator, wherein the authenticator is connected to the access server;

providing a time out feature via a card reader, wherein the card reader is connected via a network to the access server;

prompting the user to insert a game card into the card reader at an appropriate time to verify that the user is physically present at a user's geographic location;

authenticating ~~the~~ an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data via the authenticator;

identifying a first number from which the user has dialed, wherein a first number authenticating system provides anti-circumvention protection that determines a ~~physical~~ geographic location of an originating number to prevent ~~a~~ the user from connecting to the access server from a ~~physical~~ geographic location other than the user's geographic location, and wherein the first number authenticating system relies on user input and does not rely on GPS; and

determining in the authenticator whether to enable the user to access the application server based on the authenticating of the user's geographic location.

49. (original) The method of claim 48, wherein the authenticator comprises an authenticating server, and wherein authenticating further comprises authenticating through the authenticating server.

50. (canceled)

51. (canceled)

52. (original) The method of claim 48, further comprising enabling the user to request remote access to the application server through the user request enabling means.

53. (original) The method of claim 48, further comprising interconnecting the access server and the authenticating means through a network.

54. (currently amended) The method of claim 49, wherein authenticating the geographic location comprises authenticating through an authorized geographic location database.

55. (currently amended) The method of claim 49, wherein authenticating the geographic location further comprises authenticating through a RADIUS server.

56. (canceled)

57. (canceled)

58. (original) The method of claim 52, wherein enabling further comprises enabling the user request through an interface station.

59. (original) The method of claim 52, wherein enabling further comprises enabling the user request through a client.

60. (currently amended) The method of claim 52, wherein enabling further comprises enabling the user request through the geographic location identifier.

61. (canceled)

62. (currently amended) The method of claim 52, wherein authenticating the geographic location comprises authenticating the user's geographic location through a user associated identifier.

63. (original) The method of claim 52, wherein enabling comprises enabling through a dialer having an associated number.

64. (original) The method of claim 52, wherein interconnecting comprises interconnecting a plurality of user request enabling means through a plurality of local area networks.

65. (original) The method of claim 52, wherein interconnecting further comprises interconnecting with a user request enabling means.

66. (original) The method of claim 53, wherein the network comprises an intranet, and wherein interconnecting further comprises interconnecting through the intranet.

67. (original) The method of claim 53, wherein the network comprises the Internet, and wherein interconnecting further comprises interconnecting through the Internet.

68. (currently amended) The method of claim 55, wherein authenticating the identity of the user further comprises issuing a security challenge to the user request enabling means through an authenticating server.

69. (currently amended) The method of claim 62, wherein authenticating the geographic location further comprises authenticating through a locating identifier cookie.

70. (currently amended) The method of claim 63, wherein the authenticator comprises means for identifying the number associated with the dialer located at the user's geographic location, and wherein the step of authenticating the geographic location further comprises identifying the number associated with the dialer.

71. (currently amended) The method of claim 63 wherein a dialing system includes a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each associated with a different user geographic location, and the authenticator comprises means for identifying the first number dialed in the dialing system, and wherein the step of authenticating further comprises identifying the first number dialed.

72. (original) The method of claim 67, wherein the locating identifier comprises a dynamic cookie.

73. (original) The method of claim 68, wherein the user request enabling means are adapted to issue a response to the security challenge, and the authenticator include a database for enabling verification of the response of the user request enabling means to the security challenge,

and wherein the step of authenticating further comprises verifying the response to the security challenge through the verification database.

74. (original) The method of claim 70, wherein identifying further comprises identifying through Automatic Number Identification.

75. (original) The method of claim 71, wherein the step of identifying further comprises identifying through Dialed Number Identification Services.

76. (original) The method of claim 73, wherein the authenticator is further adapted to verify the response of the user request enabling means to the security challenge based on the database in the authenticator, and to authorize access to the application server, and further comprising the step of authorizing access to an application server.

77. (withdrawn) A jurisdiction verification system, comprising:

an application server;

an authentication server; and

an access server, wherein the access server is disposed remote to a client device, and wherein the access server is adapted to communicate information between the client device and the authentication server;

the authentication server adapted to issue a challenge based on a request from the client device to access the application server and to receive a response based on the challenge, the response including information provided by a user at the client device, and wherein the information does not include GPS information, so as to determine a geographic location of the client device based on the response.

78. (withdrawn) The jurisdiction verification system of claim 77, wherein the application server is adapted to accept wager-based transactions, and wherein the authentication server is further adapted to authorize communication between the client device and the application server based on the response.

79. (withdrawn) The jurisdiction verification system of claim 77, wherein the application server is adapted to accept wager-based transactions, the response includes a geographic

identifier, and the authentication server is further adapted to authorize communication between the client device and the application server if the geographic identifier is indicative of a predetermined geographic location.

80. (withdrawn) The jurisdiction verification system of claim 79, wherein the predetermined geographic location is within a jurisdiction that allows wager-based transactions.

81. (withdrawn) The jurisdiction verification system of claim 79, wherein the predetermined geographic location is within a jurisdiction that allows remote wager-based transactions.

82. (withdrawn) The jurisdiction verification system of claim 79, wherein the predetermined geographic location is within a jurisdiction that allows wager-based transactions from the predetermined geographic location to another geographic location within another jurisdiction.

83. (withdrawn) The jurisdiction verification system of claim 82, wherein the geographic identifier includes ANI information.

84. (withdrawn) The jurisdiction verification system of claim 82, wherein the geographic identifier includes an IP address.